Amendments to the Drawings

The attached sheets of drawings include changes to FIGS. 2-9A. In FIGS. 2-4, reference characters have been added. In FIGS. 4-6, reference characters have been deleted. In FIGS. 7-9A, spelling errors have been corrected. The replacements sheets 2/13 to 9/13 replace the original sheets 2/13 to 9/13.

Attachments: Eight Replacement Sheets 2/13 to 9/13
Eight Annotated Sheets 2/13 to 9/13

REMARKS

Applicants have thoroughly considered the Examiner's remarks in the September 11, 2007 Office action and have amended the application to more clearly set forth aspects of the invention. This Amendment A amends claims 1, 3, 4, 6-9, 11, 12, 14, 17, 20, 21, 23-25, and 27-29. Claims 2, 5, 13, 15, 16, 18, 19, 22, 26, 31, and 32 have been canceled.

Claims 1, 3, 4, 6-12, 14, 17, 20, 21, 23-25, and 27-30 are thus presented in the application for further examination. Reconsideration of the application as amended and in view of the following remarks is respectfully requested.

Applicants request that the Examiner now have the drawings as originally filed reviewed and accepted.

Objections

A. Drawings

Submitted with this Amendment A are Replacement Sheets 2/13-9/13, which include amendments to FIGS. 2-9A. In particular, Applicants have amended the drawings to correct misspellings in FIGS. 7-9A and to clarify items 702, 704, and 706 in FIG. 7 by adding arrows to link the items. Regarding objections for failing to comply with 37 CFR 1.84(p)(4) and (5), Applicants have amended the drawings to delete reference characters 224 and 218 and add reference characters 419, 420, 500, and 600. Original sheets 1/13 and 10/13-13/13 have not been amended by this Amendment A.

Regarding the remaining objections for failing to comply with 37 CFR 1.84(p)(5), Applicants have amended the specification to delete reference characters 224, 308, 314, and 907 and add reference character 100. In view of the foregoing, Applicants submit that the amended drawings are in proper condition for acceptance, and respectfully request that the Office review and formally accept the amended drawings.

B. Specification

As amended, the Abstract now contains fewer than 150 words. Also, Applicants have amended the specification as suggested by the Examiner. In particular, Applicants have clarified the trademark status of the term "RC4"and corrected minor grammatical and typographical errors throughout the specification. Additionally, as noted above, Applicants have amended the

specification to consistently reflect the drawings. Applicants respectfully request reconsideration and withdrawal of the objections to the specification.

C. Claim 28

As amended, claim 28 no longer includes the misspelling of the word "retrieved." Accordingly, Applicants respectfully request reconsideration and withdrawal of the objection to claim 28.

Claim Rejections Under U.S.C. §101

Claims 11, 21-24, 31, and 32 stand rejected under 35 U.S.C. §101 as being directed to non-statutory matter. The Office asserts that the "computer-readable media" referred to by claim 11 and the "computer-readable medium" referred to by claims 21-24, 31, and 32 encompasses intangible communications media making the claims non-statutory. (Office action, page 5). Applicants respectfully disagree, and assert that carrier waves, data signals, and other so-called intangible communications media are statutory subject matter. A signal encoded with functionally descriptive material is similar to a computer readable medium encoded with functionally descriptive material, both of which are capable of a functional interrelationship with a computer.

However, to advance prosecution, Applicants have amended claim 11 to recite "computer ***storage*** media." Similarly, Applicants have amended claims 21, 23, and 24 to recite "computer ***storage*** medium." Applicants point to the specification at pages 17, paragraph [0061] to page 18, paragraph [0064] for support of these amendments. Claims 22, 31 and 32 have been canceled. In view of the foregoing, Applicants respectfully submit that amended claims 11, 21, 23, and 24 are patentable subject matter within the scope of 35 U.S.C. §101.

Claim rejections under 35 U.S.C. §112, second paragraph

Claims 25-30 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Amended claim 25 no longer includes the reference to "the wrapping key" asserted by the Office. (Office action, page 5). Accordingly, Applicants respectfully

request that the Office withdraw the rejection independent claim 25 and the rejection of claims 26-30 which depend from claim 25.

Claim Rejections Under 35 U.S.C. §102(b) and 35 U.S.C. §103(a)

Claims 1-4, 11-15, 21-24, 31, and 32 stand rejected under 35 U.S.C. §102(b) as being anticipated by or, in the alternative, under 35 U.S.C. §103(a) as obvious over U.S. Patent No. 6,160,891 to Al-Salqan. Claims 10 and 25-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,160,891 to Al-Salqan. Claims 5-9, 16-20, and 28-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,160,891 to Al-Salqan and further in view of Maher, "Crypto Backup and Key Escrow," Communications of the ACM, Volume 39, Issue 3, pp. 48-53, 1996. Applicants respectfully disagree. None of the cited references, alone or in combination, disclose or suggest each and every feature claimed in the rejected claims.

Claim 1 is directed to a method of communicating private data between first and second client computers which are coupled to a data communication network. According to amended claim 1, in response to a request from a user of the first client to roam a private key, the first client generates a recovery key and a wrapping key and encrypts the private key, the recovery key and the wrapping key. In particular, the private key is encrypted as a function of the wrapping key, the wrapping key is generated as a function of an encryption password provided by the user and encrypted as a function of the recovery key, and the recovery key is encrypted as a function of the wrapping key. The first client transfers the plurality of encrypted keys (private, wrapping, and recovery keys) to a network server coupled to the data communication network. The server receives the plurality of encrypted keys and, in response, generates a backup key. The server stores the received plurality of encrypted keys and the backup key. The recovery key and the wrapping key are unknown to the network sever.

Further, amended claim 1 sets forth the user's ability to select a particular one or more computers on the computer network from which the encrypted private key can be decrypted without subsequently requiring the user's encryption password. In particular, the server receives a request from the second client for back up data and in response to the received request transfers the encrypted recovery key and the backup key from the server to the second client. The second client then receives the encryption password for decrypting the encrypted recovery key and

generates a backup encrypted recovery key representative of the recovery key encrypted as a function of the transferred backup key. The second client stores the backup recovery key so that the private key can subsequently be decrypted on the second client without the use of the user's encryption password.

As amended, claim 1 highlights that that present invention allows a user to independently enable and exclusively control recovery of the private key on roaming client computers from a single copy of the private key stored on the server. Specifically, only client computers to which the user has provided an encryption password may subsequently recover the private key from the copy stored on the server. Thus, the user defines and exclusively controls roaming access to the user's private key.

In contrast, Al-Salqan is directed to a recovery system and method that allows parties other than the principal (i.e., user) to access the private key without permission from the principal. Al-Salqan explains that the system and method disclosed therein is used "for example, if the principal leaves employment of an organization that continues to receive messages encrypted using the former employee's public key, or the organization wishes to decode information stored by the former employee and encrypted using a key known to the former employee" (Col. 6, lines 7-14).

According to Al-Salqan, private information of the principal such as mother's maiden name and social security number is encoded, for example by hashing. (Col. 4, lines 4-7, lines 33-34). In a first encryption, the result of this encoding is used to symmetrically encrypt the principal's private key or key password. (Col. 4, lines 47-52). In a second encryption, the encrypted private key or password is asymmetrically encrypted using a key received from and stored in a key storage. (Col. 4, lines 62-65). For example, the key is the public key of a trusted party such as the certificate authority that issued the principal's private key or key password. (Col. 3 line 66 to col. 4, line 1). The resulting encryption of the encrypted private key or password is referred to as the key recovery file. (Col. 5, line 1). The key recovery file is provided to and stored by the principal or others to retrieve the key encrypted therein. (Col. 5, lines 4-6; col 7, lines 7-10). The private information needed to decrypt the key recovery file can be overridden so that the key can be recovered if a user provides identity verifying information. (Col. 6, lines 15-20). For example, the user (e.g., the principal's employer) may provide the name of a company and a sworn statement in order to recover the file. (Col. 7 lines 31-34).

This is completely different from the present invention recited by claim 1. As correctly noted by the Office, Al-Salqan fails to teach generating a backup key. (Office action, page 9). As such, Al-Salqan fails to teach the encryption and recovery scheme recited by claim 1. In particular, Al-Salqan fails to teach transferring the backup key and the encrypted recovery key to the roaming client computer in response to a user's request to enable roaming recovery of the private key. As such, Al-Salqan fails to teach user enabled roaming recovery of the private key from a single stored copy of the encrypted private key stored on a server to which the encryption scheme is unknown. In fact, Al-Salqan teaches away the present invention by teaching that the key recovery file is stored by the principal and non-principals having the ability to override the encryption scheme.

Maher fails to cure the deficiencies of Al-Salqan. Maher, like Al-Salqan, is directed to a system, (i.e., "Crypto-Backup System") for decrypting files and messages that contain valuable corporate assets when the owner of the key is unavailable. (Page 48). The Crypo-Backup System consists of six components including a "Trusted Backup Agent." (Page 50). The "Trusted Backup Agent" is another user who recovers the owner's key. (Page 49, 50). For example, "Alice cannot access her key file. She has several encrypted documents she must use immediately. She runs a Crypto Backup program on them to extract the BRVs to recognize the backup agent as Bob and to send the BRVs in a package to Bob. Bob gets the package and the Crypto Back-up program extracts the encryption keys, encrypts them, and sends them back to Alice." (Page 49). Thus Maher fails to teach a user-controlled recovery backup scheme. In fact, Maher teaches away from the present invention by teaching that the recovery of an owner's key is controlled by another user.

Thus, Al-Salqan and Maher, alone and in combination fail to disclose or suggest each and every limitation of claim 1. As such, the cited references fail to provide advantages associated with the present invention. For example, as noted by the present application, the present invention allows users having an encryption password to roam private information between clients linked to a server without the server having knowledge of or ever receiving the private information. (Application, paragraph [0003]). Additionally, users having an encryption password can enable a roaming computer to recover private information. Thus, the user may roam and recover private information without depending on any other users and without any other users having access to the private information. Thus, the present invention greatly

enhances network security and significantly reduces the ability of malicious users to interfere with secure communications. (Application, paragraph [0003]).

In view of the foregoing, Applicants submit that claim 1 is patentable and respectfully submit that the rejection of claim 1 under 35 U.S.C. §103(a) should be withdrawn. Claims 12, 21, and 25 include limitations similar to those of claim 1 for recovering a private key. Accordingly, Applicants submit that claims 12, 21, and 25 are allowable for at least the same reasons that claim 1 is allowable. In addition, Applicants submit that the claims that depend from independent claims 1, 12, 21, and 25 are allowable for at least the reasons that the independent claims from which they depend are allowable.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. Applicants thus respectfully submit that claims 1, 3, 4, 6-12, 14, 17, 20, 21, 23-25, and 27-30 as presented are in condition for allowance and respectfully request favorable reconsideration of this application.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

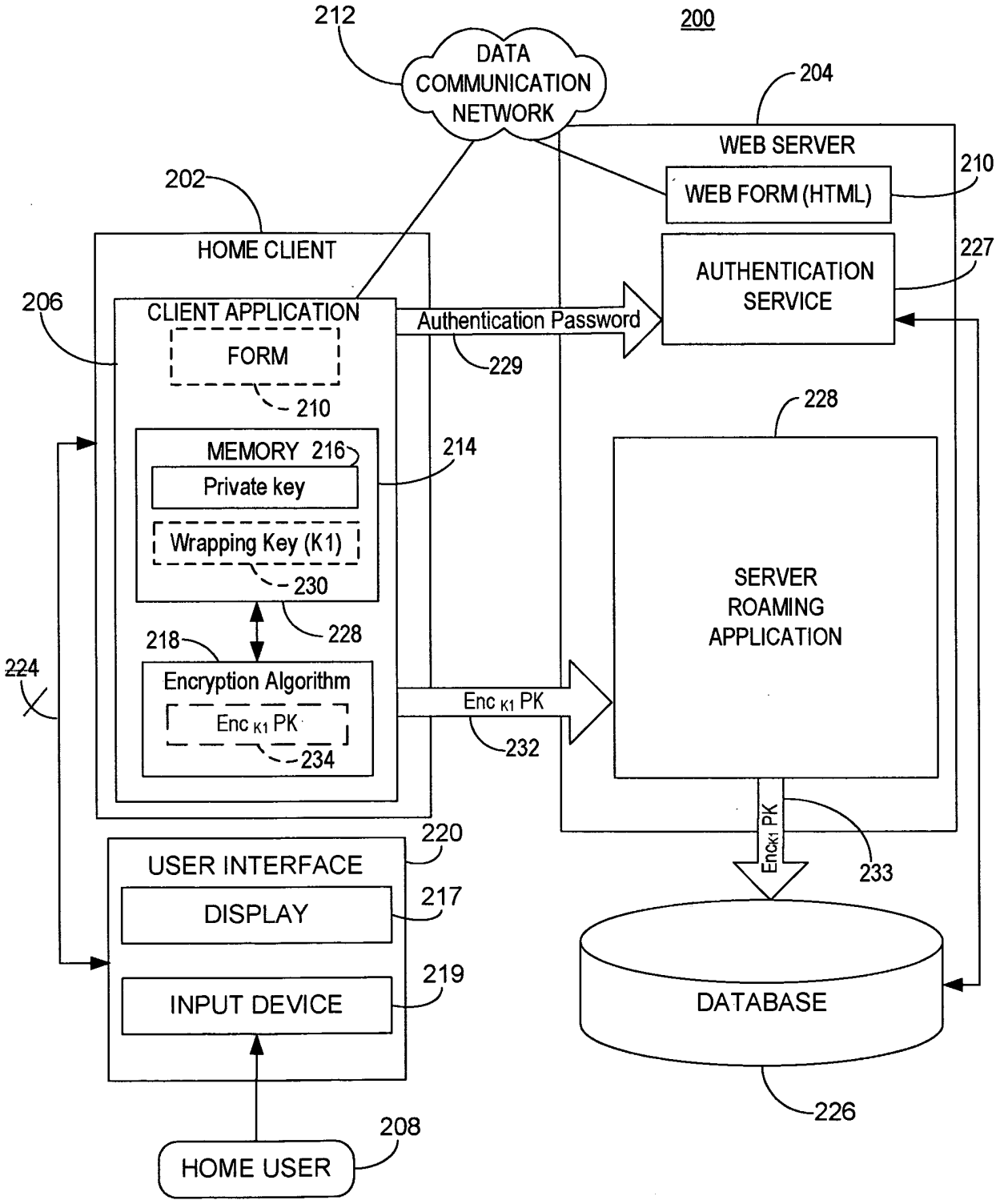
Respectfully submitted,

Robert M. Bain, Reg. No. 36,736
SENNIGER POWERS
One Metropolitan Square, 16th Floor
St. Louis, Missouri 63102
(314) 231-5400

RMB/NAS

ANNOTATED SHEET

FIG. 2



ANNOTATED SHEET

FIG. 3

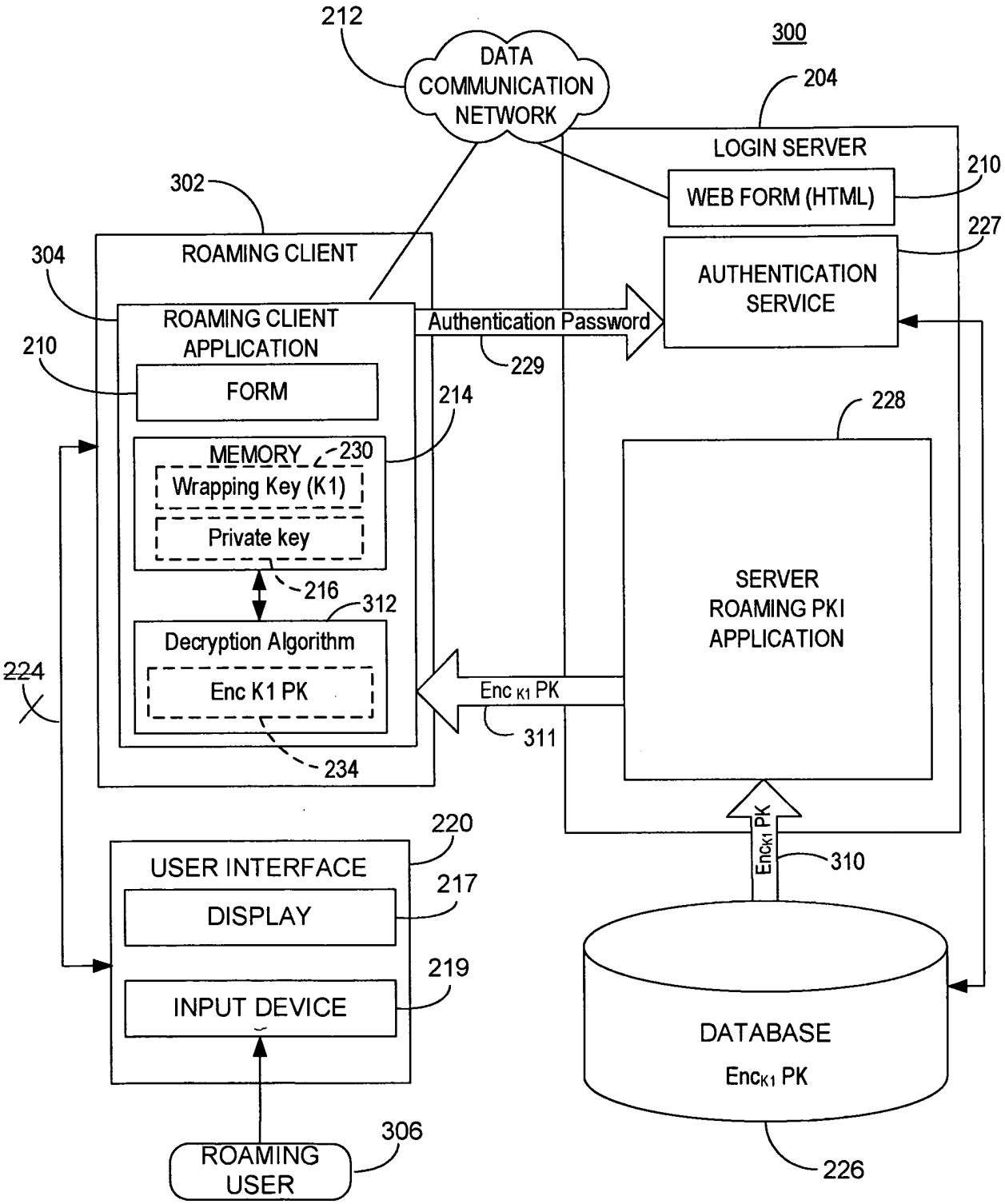


FIG. 4 ANNOTATED SHEET

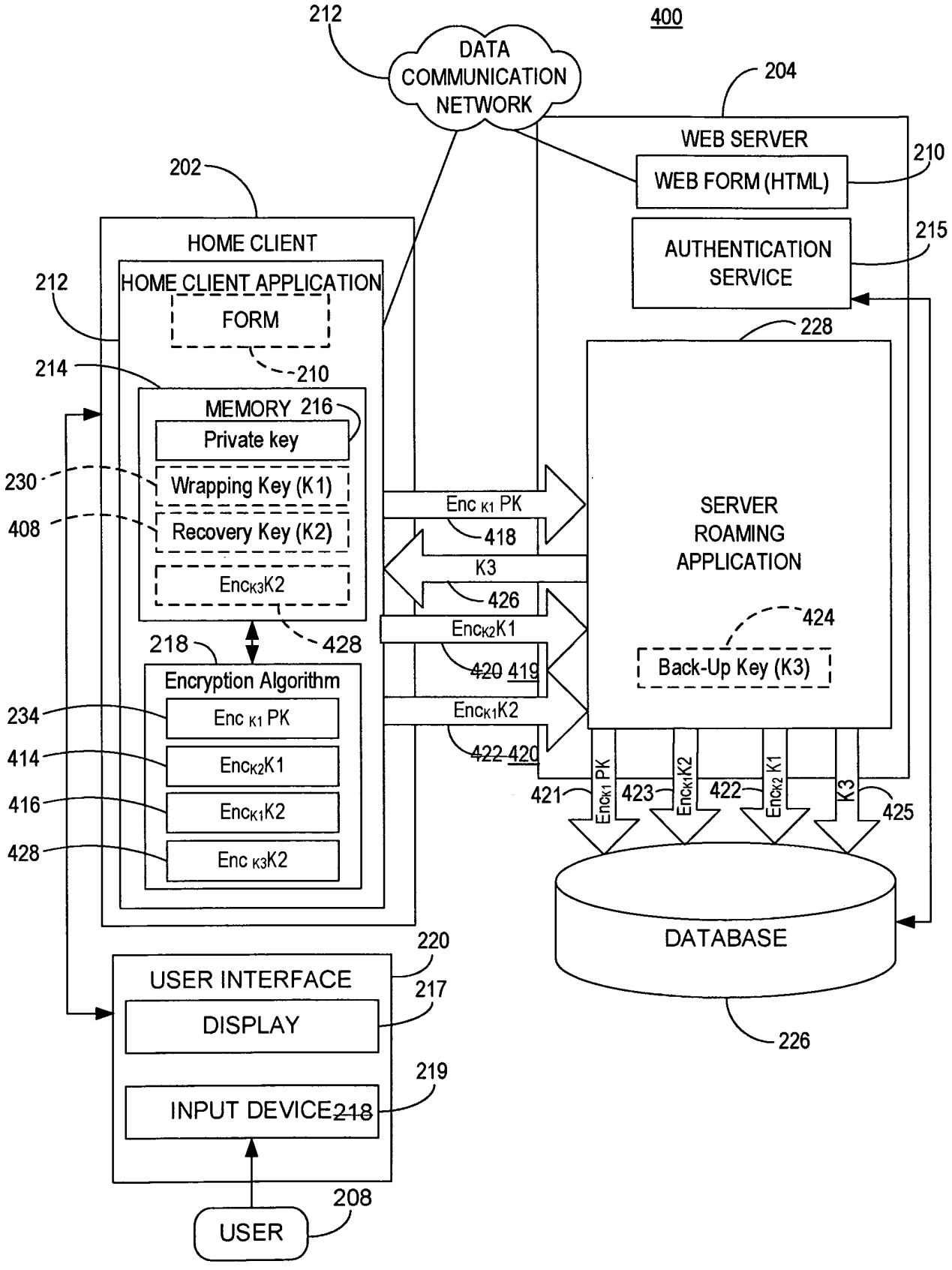
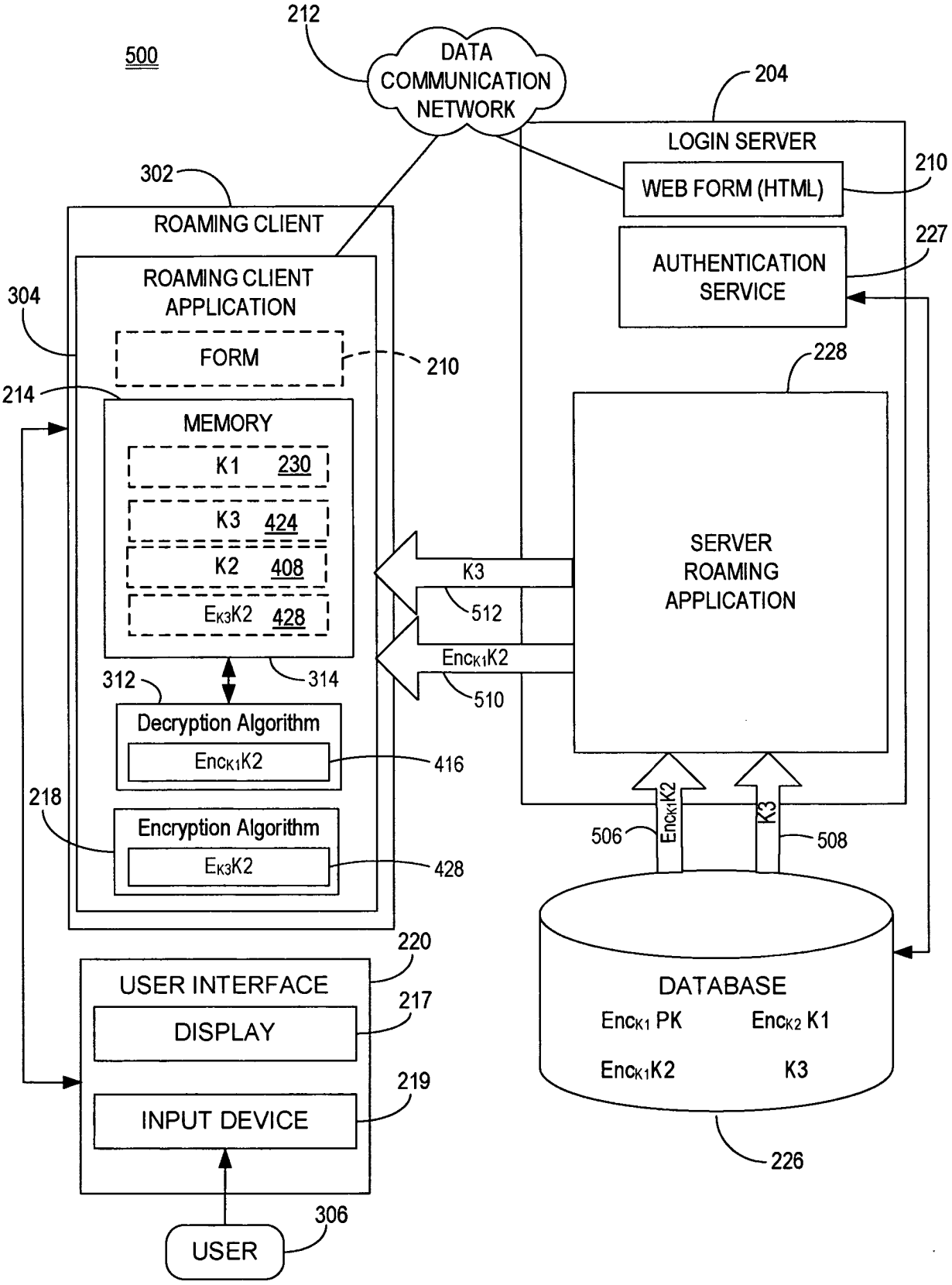


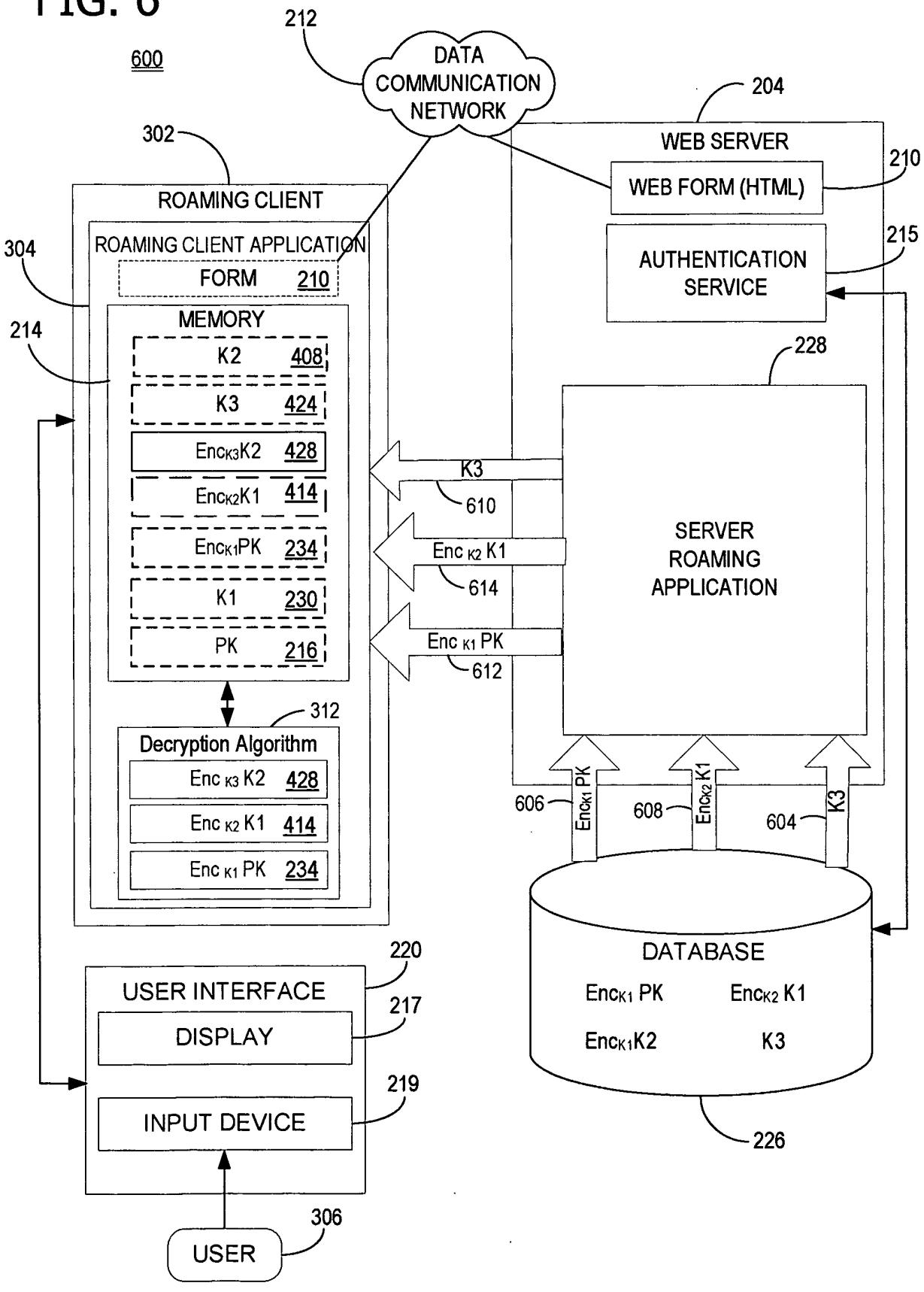
FIG. 5

ANNOTATED SHEET



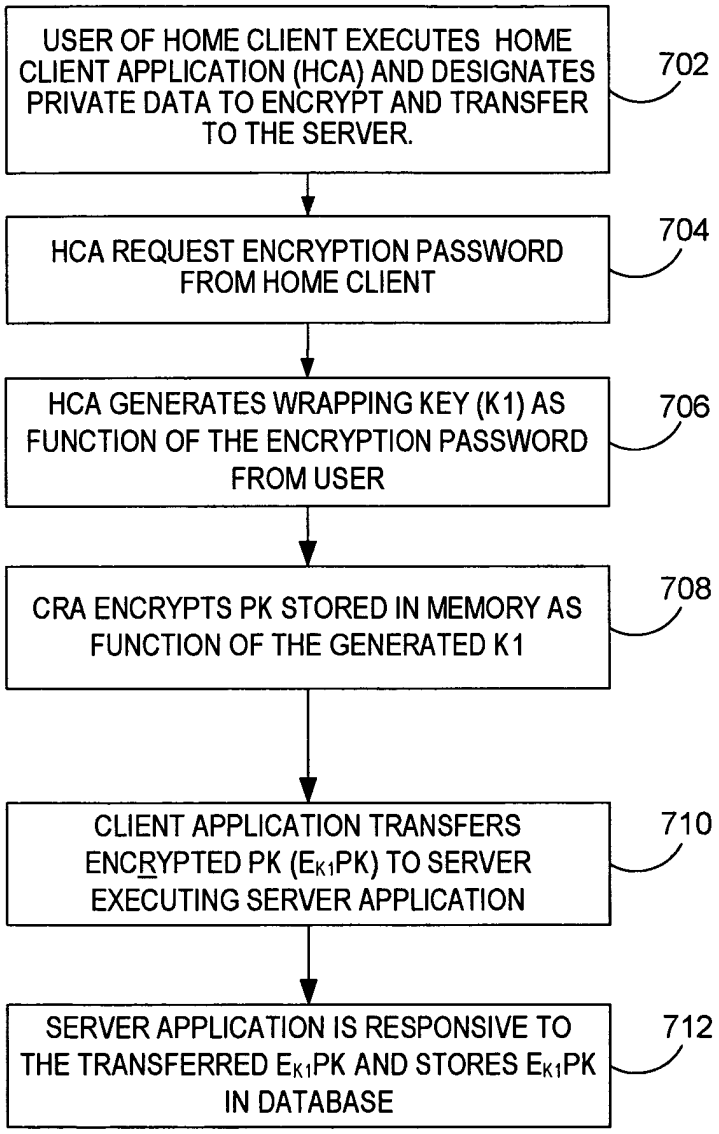
ANNOTATED SHEET

FIG. 6



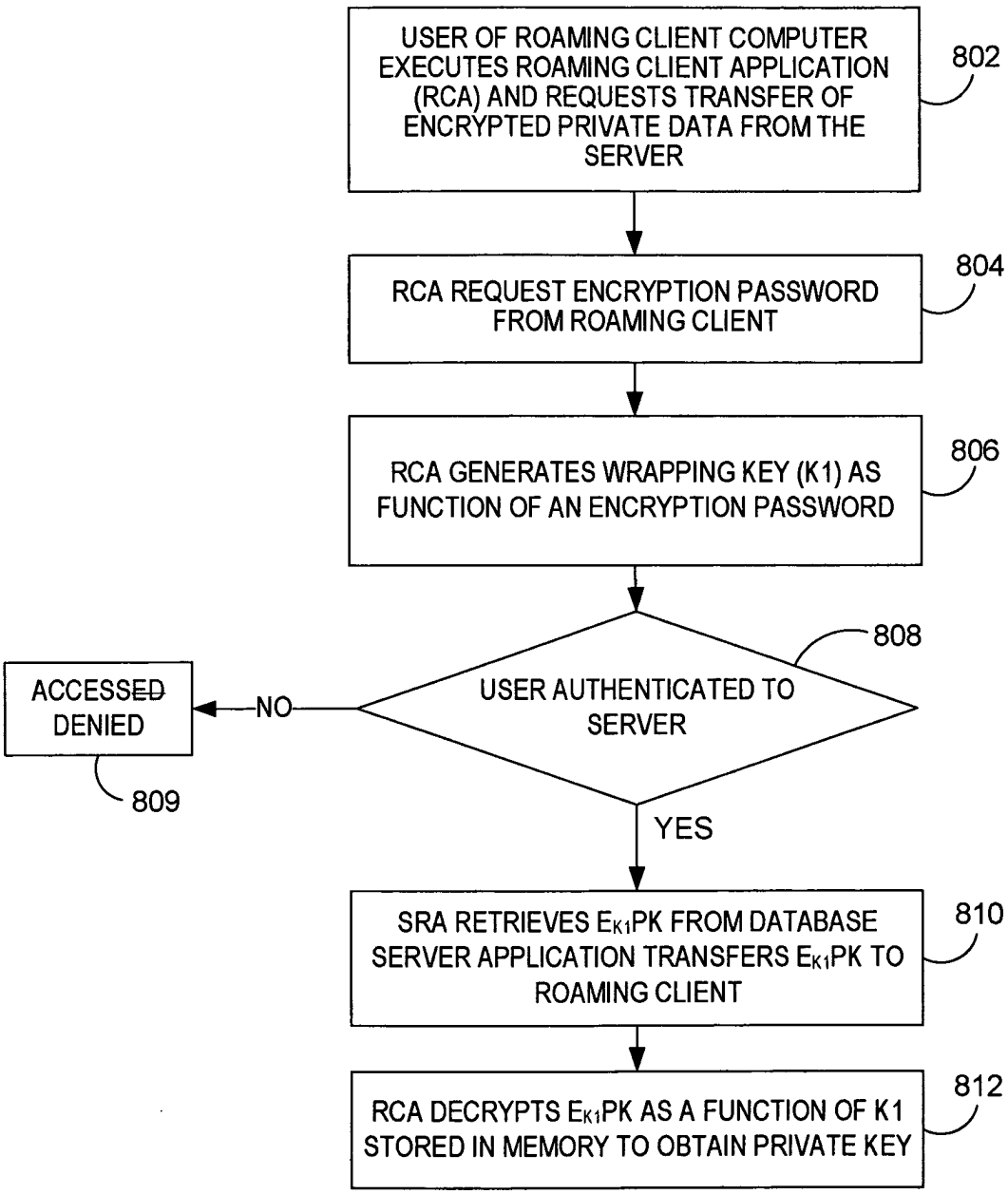
ANNOTATED SHEET

FIG. 7



ANNOTATED SHEET

FIG. 8



ANNOTATED SHEET

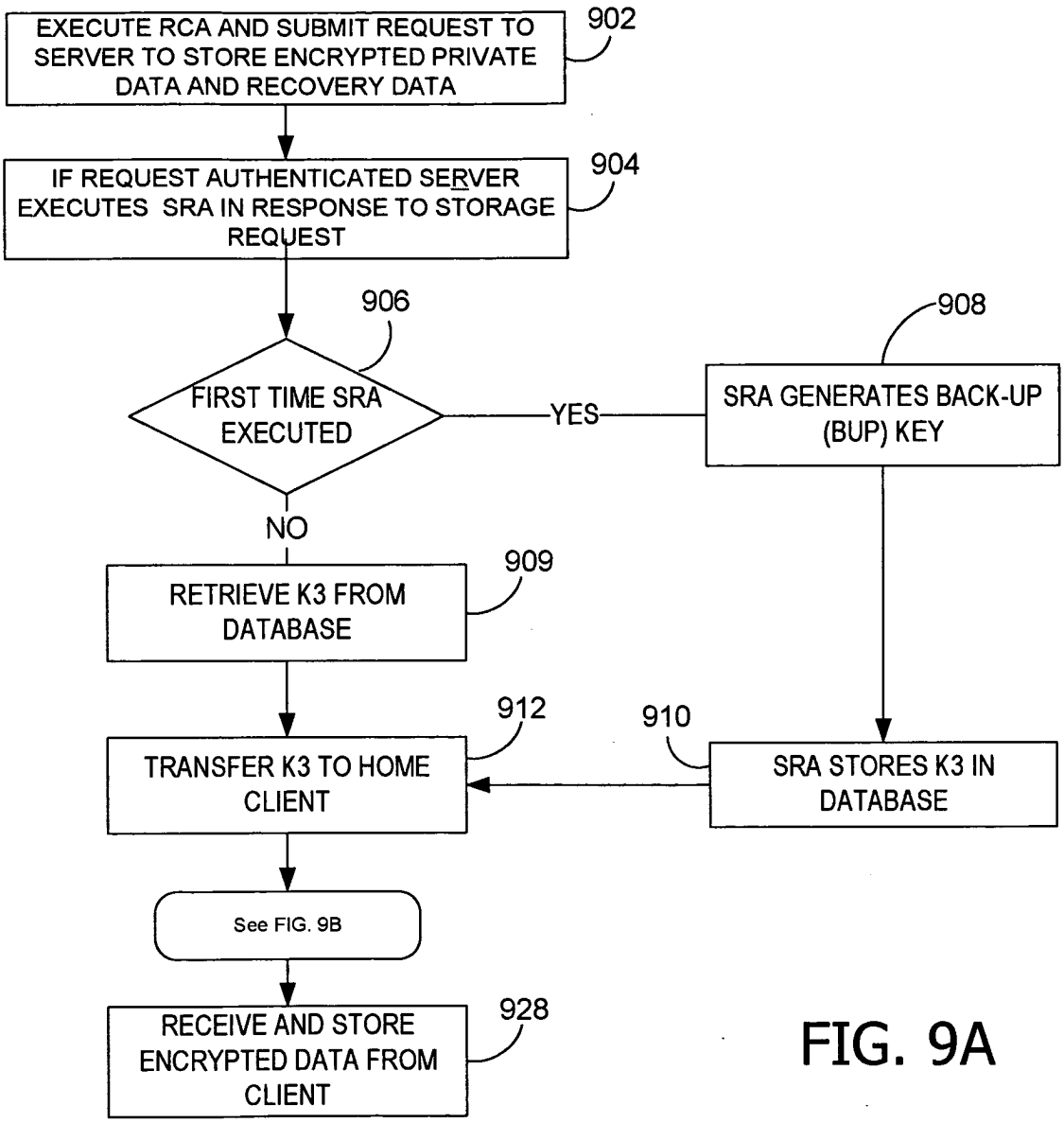


FIG. 9A